OUTLINE SHEET 5.2

Destruction

REFERENCES

SECNAV M-5510.36, Chapters 2 and 10
IA Pub P-5239-26, Remanence Security Guidebook
SECNAV M-5210.1, Records Management Manual

OUTLINE

A. Basic Policy (ISP 10-17)

1. Destruction of unneeded classified information is essential to an effective command security program

2. Destruction of record classified information

   SECNAVINST M-5210.1, Records Management Manual, includes information to determine what record information is and on retention/transfer of record information to Federal Records Centers

3. Destroy non-record classified information per SECNAV M-5510.36

4. Benefits of reducing classified holdings

   - Allows for better protection
   - Reduces storage needed
   - Reduces administrative workload
   - Better prepared for emergency

5. Classified records "Clean out" day – COs should establish to destroy unneeded classified and controlled unclassified holdings

6. For destruction of special types of classified information refer to the applicable guidance for those programs

B. Destruction Procedures (ISP 10-19)

1. Use only authorized means and personnel cleared to level of information being destroyed

2. Destruction records

   a. Secret and Confidential information – require no record of destruction except for special types of classified information; however administrative procedures for recording destruction must be established

   b. For Top Secret, record required - Can use:

      (1) OPNAV Form 5511/12, Classified Material Destruction (see Student CD for form) or any other record (e.g., log book or computerized log) that:

      - Fully identifies material
      - Shows number of copies destroyed
      - Is signed by 2 cleared witnesses
      - Shows date of destruction

      (2) Retain Top Secret record 5 years **(ISP 2-3)**

      NOTE: Record of destruction not required for Top Secret waste products (TS working papers are not considered "waste products"

3. Burn bags – Used if classified information cannot be immediately destroyed at the command. Ensure adequate storage in GSA approved storage facilities prior to destruction

   a. Striped burn bags (although not required), marked and stored according to classification level until actually destroyed, are useful in that they identify contents as classified; other types of bags should be properly marked so as to not be mistaken for trash

   b. Seal and safeguard bags awaiting destruction at level of classified information they contain

   c. Use an enclosed vehicle to transport burn bags for destruction

4. Requirements for destruction detail personnel

   - Cleared
   - Familiar with regulations and procedures
   - Trained (equipment operating procedures, emergencies, cleanup)
   - Rotated periodically

C. Methods of Destruction (ISP 10-18)

1. Use method that prevents later recognition or reconstruction

2. Methods

   a. Burning

   b. Crosscut shredder

      (1) Shreds to no greater than 5 square millimeters

          NOTE: Must be purchased from NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders (see www.navysecurity.navy.mil for latest information on crosscut shredders)

      (2) Crosscut shredders meeting old specs (3/64" x 1/2") purchased prior to 1 Jan 03 may still be used until Oct 08 if residue is "stirred" or "agitated" prior to disposal

      (3) Some special programs require more stringent control of shred residue, e.g., burning, mixing with soap/water, or mixing with unclassified residue.

   c. Pulverizers and disintegrators – Residue shall not exceed 5 square millimeters in size

   d. Mutilation - Rendering the information permanently destroyed

   e. Chemical Decomposition - Using chemicals to render the information permanently destroyed

   f. Pulping (wet process) 1/4" or smaller security screen - used for water-soluble material

3. Selecting destruction equipment

   Does it meet shred size specs?
   Does it meet safety standards?
   Does it meet local pollution standards?
   What are maintenance requirements?
   Is it simple to use?
   Will it meet requirements?
   Can you substantiate/justify cost?

D. Destruction of Non-Paper Classified information

1. IT media **(IT Pub P-5239-26, Remanence Security Guidebook)**

   NOTE: "Declassifying" magnetic media – The process by which classified information no longer requires protection.

   a. Declassifying a hard drive

      (1) Use a utility program to make three overwrites of the file - first overwrite with 1's, then 0's, and then random 1's & 0's

      (2) For inoperative equipment - Degauss with authorized degausser

      (3) Required when the media will be released outside the command for repair, turn-in, or release to another facility

      NOTE: These methods are not authorized for USMC Commands (MARADMIN 044/02)

   b. Hard drives containing classified data may be sent to NSA for destruction. The address is listed in paragraph 4 below. Any questions can be directed to Customer Service (301) 688-6672

   c. Floppy disks - Destroy by incineration, or remove outer cover and shred the internal disk with cross cut shredder or pulverizer. Mix material with paper to lessen the chance of clogging machine

      NOTE: May also use Degausser/Eraser equipment

   d. Magnetic tapes - Remove classified information by degaussing (exposing tape to a magnetic force) Degaussing devices are approved by National Security Agency and available through the National Supply System

   e. Monitors - Cathode Ray Tubes (CRT). If images of classified information are etched into the CRT phosphor refer to IA Pub P-5239-26

2. Equipment - Remove the classified component and store in security container until properly destroyed

3. Film and negatives – Incinerate, shred through an approved crosscut shredder, or pulverize

4. CD Media **(IA Pub P-5239-26)**

   a. Approved equipment can be purchased off the GSA schedule for destruction of CDs

      NOTE: Only an approved CD declassifier may be used to remove classified data bearing surfaces. Classified CDs may not be broken up.

   b. CDs can also be transmitted to NSA for destruction at no cost to commands:

      Top Secret - CD media may be transmitted via the Defense Courier Service to the following account/ address for destruction:

      DCS
      HKD093
      449276 BA21 021
      DIRNSA FT MEADE MD

      Secret, Confidential, and Unclassified – CD media may be transmitted via appropriate means to the following address for destruction:

      National Security Agency
      Attn: CMC-Degaussing
      Suite 6875
      9800 Savage Rd.,
      Ft. Meade, MD 20755-6875

      See website http://www.nsa.gov\cmc for guidance on shipping, receipt requirement (CMC Procedures and Forms) and other services provided by NSA'S Classified Material Conversion

E. Destruction of Controlled Unclassified Material (ISP 10-20)

1. Destroy SBU, DOD UCNI, DOE UCNI, FOUO, and technical documents by any means approved for the destruction of classified information or by any means that would make it difficult to recognize or reconstruct the information – Records of destruction not required

2. IT storage media containing digital FOUO, SBU, DOD UNCI and unclassified technical documents shall, at a minimum, be reformatted prior to reuse within a DOD IT system

3. Destroy unclassified NNPI in same manner approved for classified information

F. Commands Removed from Active Status (ISP 10-21)

1. Dispose of classified information by approved means or store at approved facility if status is temporary

2. CO will certify to accepting command that:

   a. Security Inspection conducted and all classified information has been removed, and

   b. Provide documentation for information left aboard

G. Emergency Destruction Supplement (ISP Exhibit 2B Part Two)

1. Required for command emergency plans for commands located outside the U.S. and its territories and deployable units

   NOTE: For COMSEC information, refer to CMS/EKMS program guidance

2. Factors to be considered in planning

   - Volume and sensitivity of information held
   - Proximity to hostile forces
   - Need to remain operational

3. Formalizing an Emergency Destruction Supplement

   a. Be specific - list procedures and methods to be used (e.g., evacuation/relocation, emergency destruction equipment, etc.)

   b. Identify exact locations of classified information, including specific drawers, shelves, sections of security containers

   c. Establish destruction priorities

      Priority 1 - Top Secret (includes all categories; destroy any special program material first, then GENSER)

      If time allows, destroy Priority 2 (Secret) special program then GENSER, and Priority 3 (Confidential) special program then GENSER

NOTE: Jettisoning or sinking are methods that can be used in an emergency

d. Be specific in tasking - Use billet designations; e.g., Admin Officer will...

e. Establish reporting requirements to account for material destroyed/not destroyed; make report to CNO (N09N2) and Admin chain of command

f. Conduct drills as necessary to train personnel

4. Naval surface noncombatant vessels operating in hostile areas without escort shall have appropriate equipment on board prepared for use

5. Measures to precede emergency destruction planning

a. Reduce amount of classified information to minimum

b. Store infrequently used information at a more secure command

c. Transfer to magnetic media or CD

(1) Reduces bulk; saves space

(2) Easier to destroy